

A FORMULATION FOR p -ADIC VERSIONS OF THE BIRCH AND SWINNERTON-DYER CONJECTURES IN THE SUPERSINGULAR CASE

FLORIAN E. I. SPRUNG

1. INTRODUCTION

Let E be an elliptic curve over the rational numbers \mathbb{Q} . The \mathbb{Q} -rational points form a finitely generated abelian group $E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$, and the classical Birch and Swinnerton-Dyer conjectures predict that the order of vanishing r_C^{an} of the Hasse-Weil L -function $L(E, s)$ at $s = 1$, an analytic quantity, should be equal to r , an algebraic quantity. The second part of their conjecture says that the leading Taylor coefficient of $L(E, s)$ should encode $E(\mathbb{Q})_{tors}$ and the size of the Tate-Shafarevich group $\text{III}(E/\mathbb{Q})$, among other algebraic quantities. More precisely, this conjecture says the following.

Denote by $\omega = \omega_E$ the Néron differential and by $\Omega_E = \int_{E(\mathbb{R})} \omega \in \mathbb{R}^{>0}$ the Néron period of E . We denote by $L^*(E)$ the leading coefficient of the Taylor expansion at $s = 1$.

Conjecture 1.1 (BSD).

- (1) We have $r_C^{an} = r$.
- (2)
$$\frac{L^*(E)}{\Omega_E} = \frac{\prod_v c_v \cdot \#\text{III}(E/\mathbb{Q}) \cdot \text{Reg}_{\mathbb{C}}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2}.$$

Here, c_v denotes the Tamagawa number for a place v , and the regulator $\text{Reg}_{\mathbb{C}}(E/\mathbb{Q})$ is the discriminant of the Néron-Tate canonical height pairing on $E(\mathbb{Q})$.

To construct a p -adic analogue, we identify algebraic numbers with p -adic numbers by fixing an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$. A p -adic analogue of this conjecture should look as follows. There should be a p -adic L -function $L_p(E, T)$, whose order of vanishing r^{an} at $T = 0$ should equal r , and whose leading Taylor coefficient should again encode algebraic quantities of E including $E(\mathbb{Q})_{tors}$ and $\#\text{III}(E/\mathbb{Q})$ as in the above formula, with the regulator $\text{Reg}_{\mathbb{C}}$ replaced by a p -adic avatar. There are two types of such p -adic analogues.

The first type concerns the case when p is a prime of ordinary reduction (meaning that p is coprime to $a_p := p + 1 - \#E(\mathbb{F}_p)$). Here, Mazur, Tate, and Teitelbaum formulated a p -adic version of these conjectures. The p -adic L -function $L_p(E, T)$ they employed gave rise to the expected version of p -adic BSD when p was of good ordinary reduction, but in the split multiplicative case r^{an} corresponded to $r + 1$ in view of an extra zero.

The second type is the supersingular case (the case when $p|a_p$), which is more complex. There are *two* classical p -adic L -functions, denoted $L_{\alpha}(E, T)$ and $L_{\beta}(E, T)$, constructed independently by Amice and Vêlu, and Vishik. The subscripts α and β denote the roots of the Hecke polynomial $Y^2 - a_p Y + p$. The formulation of a p -adic analogue of the Birch

and Swinnerton-Dyer conjectures in terms of these $L_\alpha(E, T)$ and $L_\beta(E, T)$ when p is of good reduction is due to Bernardi and Perrin-Riou. For questions of formulating Birch and Swinnerton-Dyer conjectures, this seems to suggest that the picture is complete except for some primes of bad reduction. The goal of this paper is to indicate that this is not the case.

We do this by formulating p -adic versions of BSD for supersingular primes p using a more natural pair of p -adic L -functions $L_\sharp(E, T)$ and $L_b(E, T)$. This hints at a formulation of p -adic BSD in the ordinary case in terms of such a pair as well. These p -adic L -functions had been constructed by Pollack, Kobayashi, and the author in the supersingular case and are functions living in the power series ring $\mathbb{Z}_p[[T]]$, unlike $L_\alpha(E, T)$ and $L_\beta(E, T)$ which have more complicated growth properties. Apart from being an ingredient for a natural formulation of the Iwasawa Main Conjecture, the appearance of the Iwasawa invariants of this pair of p -adic L -functions indicates that this pair is the natural choice: The Iwasawa invariants appear in analytic estimates for the sizes of the p -primary parts of the Tate-Shafarevich group along the cyclotomic \mathbb{Z}_p -extensions. The term “analytic estimates” refers to the corresponding special values of the Hasse-Weil L -functions twisted by characters of p -power conductor, which should encode these sizes. These *analytic* estimates can be found in [Po03] and [Sp15]. There are algebraic counterparts of $L_\sharp(E, T)$ and $L_b(E, T)$, which are modified Selmer groups $\text{Sel}^\sharp(E)$ and $\text{Sel}^b(E)$. Using their Iwasawa invariants one can estimate these sizes directly, see e.g. [Ko03] and [Sp13]. In addition to these estimates, the Iwasawa invariants appear in upper bounds for the rank of the elliptic curve in the cyclotomic \mathbb{Z}_p -extension of \mathbb{Q} . For analytic estimates, see [Po03] and [Sp15], and for their algebraic counterparts, see [Ko03] and [Sp16].

Concretely, our conjecture says the following.

Conjecture 1.2 (Tandem p -adic BSD). *Let E be an elliptic curve and p a prime of good supersingular reduction. Denote by \vec{L}_p^* the first non-zero Taylor coefficient around $T = 0$ of the vector of p -adic L -functions $(L_\sharp(E, T), L_b(E, T))$.*

(1) *The minimum of the orders of vanishing of $L_\sharp(E, T)$ and $L_b(E, T)$ at $T = 0$ is equal*

$$(2) \quad \vec{L}_p^* = \frac{t_Q r.}{(\#E(\mathbb{Q})_{tors})^2} \text{Reg}_p^\sharp(E/\mathbb{Q}).$$

Our regulator $\text{Reg}_p^\sharp(E/\mathbb{Q})$ is constructed explicitly from height functions that mirror the construction of $L_\sharp(E, T)$ and $L_b(E, T)$.

Theorem 1.3. *This conjecture is equivalent to the conjectures of Bernardi and Perrin-Riou.*

Since we have two functions at hand, we may consider their quotient, and give the following criterion for detecting non-zero rank:

Theorem 1.4. *Assume property (*) below holds and that $\text{III}(E/\mathbb{Q})[p^\infty] < \infty$. Then*

$$\begin{aligned} \text{rank} E(\mathbb{Q}) > 0 &\iff \left. \frac{L_\sharp(E, T)}{L_b(E, T)} \right|_{T=0} \neq \frac{-a_p^2 + 2a_p + p - 1}{2 - a_p} \text{ for odd } p, \text{ and} \\ \text{rank} E(\mathbb{Q}) > 0 &\iff \left. \frac{L_\sharp(E, T)}{L_b(E, T)} \right|_{T=0} \neq \frac{-a_2^3 + 2a_2^2 + 3a_2 - 4}{-a_2^2 + 2a_2 + 1} \text{ for } p = 2. \end{aligned}$$

This theorem is a generalization of [KP07, Corollary 0.5] who assumed p to be odd and $a_p = 0$, which is automatically satisfied when $p \geq 5$. We remark that the proof of Kurihara and Pollack almost immediately generalizes once the $L_\sharp(E, T)$ and $L_b(E, T)$ have been defined in complete generality, as done in [Sp12]. There is only one proposition in their tools that assumes $a_p = 0$, which is fixed in this paper by adhering to a generalization found in [Sp13].

As a corollary to this, we get:

Corollary 1.5. *Let $\text{rank} E(\mathbb{Q}) = 0$. Then both $L_\sharp(E, T)$ and $L_b(E, T)$ are non-zero functions, confirming [Sp12, Conjecture 6.15] in this case.*

Another object to consider given two quantities is their greatest common divisor. Denote by d_n the normalized jump in ranks $\frac{1}{p^n - p^{n-1}} (\text{rank} E(\mathbb{Q}_n) - \text{rank} E(\mathbb{Q}_{n-1}))$, where \mathbb{Q}_n is the n th layer in the cyclotomic \mathbb{Z}_p -extension numbered so that $\mathbb{Q}_0 = \mathbb{Q}$. We also let Φ_{p^n} be the p^n th cyclotomic polynomial. Kurihara and Pollack have formulated the following conjecture in the case $a_p = 0$ and p odd:

Conjecture 1.6. *Let E/\mathbb{Q} be an elliptic curve, and p a good supersingular prime. Then*

$$\gcd(L_\sharp(E, T), L_b(E, T)) = \left(T^r \prod_{d_n \geq 1 \text{ and } n \geq 1} \Phi_{p^n}^{d_n-1}(1+T) \right).$$

Note that we excluded their assumptions. This is because we give some evidence towards their conjecture by proving the following proposition which works for general supersingular p . Denote by r^{an} the order of vanishing of $L(\alpha, T)$ (or $L(\beta, T)$) at $T = 0$:

Proposition 1.7. *Let E/\mathbb{Q} be an elliptic curve and p a prime of good reduction. For some polynomial $P_{\text{III}}(E, T)$ with $P_{\text{III}}(E, \zeta_{p^n} - 1) \neq 0$ for $n \geq 0$,*

$$\gcd(L_\sharp(E, T), L_b(E, T)) = \left(P_{\text{III}}(E, T) \cdot T^{r^{an}} \prod_{d_n \geq 1 \text{ and } n \geq 1} \Phi_{p^n}^{\epsilon_n^{an}-1}(1+T) \right),$$

where $\epsilon_n^{an} = d_n^{an}$ or $\epsilon_n^{an} = d_n^{an} + 1$.

Finally, we ask a question on a possible generalization of the situation to the ordinary case. When p is ordinary, the functions $L_\sharp(E, T)$ and $L_b(E, T)$ are not uniquely defined, but their values at $T = 0$ are. We find that when p is odd and $a_p = 2$, $L_b(E, 0) = 0$.

Question 1. Where does this ‘extra zero phenomenon’ in the ordinary case come from?

In [LZ13], Loeffler and Zerbes find a pair of Iwasawa functions in the ordinary case using the theory of Wach modules. The above question suggests that an extra zero phenomenon should occur in terms of their pair as well.

2. REVIEW OF p -ADIC L -FUNCTIONS FOR ELLIPTIC CURVES

Let p be a prime of good reduction for our elliptic curve E . The work of Mazur, Swinnerton-Dyer, Amice and Vélú, and Višik gives constructions of p -adic L -functions

that should encode the behavior of the \mathbb{Q}_n -rational points $E(\mathbb{Q}_n)$ of the elliptic curve E . Concretely, denote by α and β the roots of the Hecke polynomial $Y^2 - a_p Y + p$ ordered so that $\text{ord}_p(\alpha) \leq \text{ord}_p(\beta)$ for any p -adic valuation ord_p . We say that α resp. β is an allowable root if $\text{ord}_p(\alpha) < \text{ord}_p(p)$ resp. $\text{ord}_p(\beta) < \text{ord}_p(p)$. Notice that α is always allowable by convention, while β is only when p is supersingular.

Notation 2.1. We denote by ζ_{p^n} a primitive p^n th root of unity, and we let $N = n + 1$ when p is odd and $N = n + 2$ when $p = 2$. We also let χ_u be a group morphism from $1 + 2p\mathbb{Z}_p$ into \mathbb{C}_p^\times sending a topological generator $1 + 2p$ to some $u \in \mathbb{C}_p$ so that $|u - 1|_p < 1$, where $|\cdot|_p$ is the normalized p -adic absolute value (i.e. $|\frac{1}{p}|_p = 1$).

Theorem 2.2 (Mazur and Swinnerton-Dyer, Amice and Vélú, Višik). [MTT86, Proposition in Section 14] *Let E be an elliptic curve over \mathbb{Q} and p a prime of good reduction. Regard $\chi_{\zeta_{p^n}}$ and $\chi_{\zeta_{p^n}^{-1}}$ as characters of $\mathbb{Z}_p/p^n\mathbb{Z}_p$. There is a p -adic analytic function $L_\alpha(E, T)$ converging on the open unit disk with the following interpolation properties:*

$$L_\alpha(E, \zeta_{p^n} - 1) = \frac{p^N}{\alpha^N \tau(\chi_{\zeta_{p^n}^{-1}})} \frac{L(E, \chi_{\zeta_{p^n}^{-1}}, 1)}{\Omega_E}, \text{ and}$$

$$L_\alpha(E, 0) = \left(1 - \frac{1}{\alpha}\right)^2 \frac{L(E, 1)}{\Omega_E}.$$

When β is allowable (i.e. p is supersingular), there is a companion p -adic analytic function $L_\beta(E, T)$ with the same interpolation properties with α replaced by β .

While these classical $L_\alpha(E, T)$ have bounded coefficients when p is ordinary, they are not elements of $\mathbb{Z}_p[[T]]$ (or even of $\mathbb{Z}_p[[T]] \otimes \overline{\mathbb{Q}_p}$) when p is supersingular. The following theorem fixes this situation:

Theorem 2.3. [Po03, Theorem 5.6 for $a_p = 0$] [Sp12, Theorem 6.12 for general $p|a_p$] *Let p be a prime of good supersingular reduction. Then there are two p -adic L -functions $L_\#(E, T)$ and $L_b(E, T)$ which are elements of $\mathbb{Z}_p[[T]]$ so that we may write*

$$(L_\alpha(E, T), L_\beta(E, T)) = (L_\#(E, T), L_b(E, T)) \mathcal{L}og_{\alpha, \beta}(1 + T),$$

where

$$\mathcal{L}og_{\alpha, \beta}(1 + T) := \lim_{n \rightarrow \infty} \begin{pmatrix} a_p & 1 \\ \Phi_{p^1}(1+T) & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ \Phi_{p^2}(1+T) & 0 \end{pmatrix} \cdots \begin{pmatrix} a_p & 1 \\ \Phi_{p^n}(1+T) & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ p & 0 \end{pmatrix}^{-(N+1)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}$$

is a matrix of p -adic analytic functions converging on the open p -adic unit disk.

Theorem 2.4. [Sp15, Theorem 2.14] *Let p be an ordinary good prime. Then the first column \log_α of $\mathcal{L}og_{\alpha, \beta}(1 + T)$ converges and we have*

$$L_\alpha(E, T) = (L_\#(E, T), L_b(E, T)) \log_\alpha,$$

for two p -adic analytic functions converging on the closed p -adic unit disk $L_\#(E, T)$ and $L_b(E, T)$.

We remark that these $L_{\sharp}(E, T)$ and $L_{\flat}(E, T)$ are not uniquely defined in the ordinary case, but their values at $T = 0$ are unique:

Lemma 2.5. *The value of the vector $(L_{\sharp}(E, 0), L_{\flat}(E, 0))$ equals*

$$\begin{cases} (-a_p^2 + 2a_p + p - 1, -a_p + 2) \cdot \frac{L(E, 1)}{\Omega_E} & \text{when } p \text{ is odd,} \\ (-a_p^3 + 2a_p^2 + 2pa_p - a_p - 2p, -a_p^2 + 2a_p + p - 1) \cdot \frac{L(E, 1)}{\Omega_E} & \text{when } p \text{ is even.} \end{cases}$$

Proof. This follows from the table before Proposition 6.14. in [Sp12] in the supersingular case and the one before Conjecture 5.18 in [Sp15] for the general case. Q.E.D.

3. THE BEHAVIOR AT $T = 0$: A CRITERION FOR NON-ZERO RANK

The goal of this short section is to prove:

Theorem 3.1. *Assume property $(*)$ below holds and that $\text{III}(E/\mathbb{Q})[p^\infty] < \infty$. Then*

$$\begin{aligned} \text{rank} E(\mathbb{Q}) > 0 &\iff \left. \frac{L_{\sharp}(E, T)}{L_{\flat}(E, T)} \right|_{T=0} \neq \frac{-a_p^2 + 2a_p + p - 1}{2 - a_p} \text{ for odd } p, \text{ and} \\ \text{rank} E(\mathbb{Q}) > 0 &\iff \left. \frac{L_{\sharp}(E, T)}{L_{\flat}(E, T)} \right|_{T=0} \neq \frac{-a_2^3 + 2a_2^2 + 3a_2 - 4}{-a_2^2 + 2a_2 + 1} \text{ for } p = 2. \end{aligned}$$

Let $T_p(E)$ be the Tate module for E .

Here is property $(*)$: The composite of natural maps

$$\mathbf{H}_{\text{glob}}^1 = \varprojlim H_{\text{et}}^1(\mathbb{Q}_n[1/S], T_p(E)) \rightarrow H^1(\mathbb{Q}, T_p(E)) \rightarrow H^1(\mathbb{Q}_p, T_p(E))$$

is not zero. Here, the limit is taken with respect to corestriction, and S is the product of the bad reduction primes and p .

We remark that property $(*)$ should always be true.

Proof of Theorem. The arguments of Kurihara and Pollack of [KP07, Section 1.4] almost work with the appropriate modifications. In terms of notation, we write $Col(z) = (Col^{\sharp}(z), Col^{\flat}(z))$ with the Coleman maps from [Sp12] instead of the functions $h_z(T)$ and $k_z(T)$. We note that their arguments work in spite of having to take into account the possibility of one of $L_{\sharp}(E, T)$ or $L_{\flat}(E, T)$ to be zero, cf. [Sp12, 6.15] and the surrounding discussions! Finally, [KP07, Proposition 1.2] is only proved in the case $a_p = 0$. To remedy this, we refer to the isotypical component of the trivial tame character of the inverse limit of [Sp13, Proposition 4.7] and remark that the arguments found therein all apply when $p = 2$ as well. Q.E.D.

Corollary 3.2. [Sp12, Conjecture 6.15] *said that both $L_{\sharp}(E, T)$ or $L_{\flat}(E, T)$ are non-zero. This conjecture holds in the case where $\text{rank} E(\mathbb{Q}) = 0$.*

Proof. We know that at least one of $L_{\sharp}(E, T)$ or $L_{\flat}(E, T)$ is non-zero by [Sp12, Proposition 6.14], so the theorem tells us they both have to be. Q.E.D.

4. THE BEHAVIOR AT $T = 0$: p -ADIC VERSIONS OF THE BSD CONJECTURES

The goal of this section is to formulate p -adic versions of BSD in terms of the vector $(L_{\sharp}(E, T), L_b(E, T))$ in the supersingular case. We thus assume that p is supersingular for this section.

4.1. Dieudonné modules and p -adic heights. The Dieudonné module is the following two-dimensional \mathbb{Q}_p -vector space:

$$D_p(E) := \mathbb{Q}_p \otimes H_{dR}^1(E/\mathbb{Q})$$

There is a Frobenius endomorphism φ which acts on $D_p(E)$ linearly. We refer the reader to [BPR93, Paragraph 2] for a concrete definition, but let us record that its characteristic polynomial is $Y^2 - \frac{a_p}{p}Y + \frac{1}{p}$, as opposed to the definition of [MST06] or [Ke01] (where it is $Y^2 - a_pY + p$). This vector space admits a basis ω and $\varphi(\omega)$, where ω is the invariant/Néron differential of E . We want to define eigenvectors $\nu_A := \nu_{\frac{1}{\alpha}}$ and $\nu_B := \nu_{\frac{1}{\beta}}$ of φ with eigenvalues $\frac{1}{\alpha}$ and $\frac{1}{\beta}$ which live in the $\mathbb{Q}_p(\alpha)$ -vector space

$$D_p(E)(\alpha) := \mathbb{Q}_p(\alpha) \otimes H_{dR}^1(E/\mathbb{Q}).$$

Definition 4.1. We define (scale) both eigenvectors as follows:

$$\begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix} := \begin{pmatrix} -\alpha & p \\ \beta & -p \end{pmatrix} \frac{1}{\beta - \alpha} \begin{pmatrix} \omega \\ \varphi(\omega) \end{pmatrix}$$

Definition 4.2. Perrin-Riou's p -adic L -function can be defined via the classical p -adic L -functions $L_{\alpha} := L_{\alpha}(E, \alpha, T)$ and $L_{\beta} := L_{\beta}(E, \beta, T)$:

$$L_p^{PR}(E, T) := (L_{\alpha}, L_{\beta}) \begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix}$$

This is equivalent via the arguments in [SW13, Section 3.5] to Perrin-Riou's construction in [PR03, Section 2.2].

Lemma 4.3 ($D_p(E)$ -rationality of coefficients). *We have $L_p^{PR}(E, T) \in D_p(E)[[T]]$.*

Proof. By Theorem 2.3, we can write

$$L_p^{PR}(E, T) = (L_{\sharp}, L_b) \mathcal{L}og_{\alpha, \beta} \begin{pmatrix} 1 & \alpha \\ 1 & \beta \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ a_p & -p \end{pmatrix} \begin{pmatrix} \omega \\ \varphi(\omega) \end{pmatrix}.$$

From the definition of $\mathcal{L}og_{\alpha, \beta}$, we then see that $L_p^{PR}(E, T) \in D_p(E)[[T]]$, as desired. Q.E.D.

Given a globally minimal Weierstrass equation over \mathbb{Z}

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for E , recall that the associated Néron/invariant differential is $\omega = \frac{dx}{2y + a_1x + a_3}$ (see e.g. [Sil, Chapter III.1]). The \mathbb{Q} -vector space $H_{dR}^1(E/\mathbb{Q})$ admits a basis $\{\omega, x\omega\}$ and is equipped with a canonical alternating bilinear form $[\cdot, \cdot]$ so that $[\omega, x\omega] = 1$. We extend it linearly to the Dieudonné modules above and denote these extensions by $[\cdot, \cdot]$ as well.

Fix ω . Then for each $\nu \in D_p(E)$ (resp. $\nu \in D_p(E)(\alpha)$), one can associate a quadratic form h_ν mapping $E(\mathbb{Q})$ to \mathbb{Q}_p (resp. to $\mathbb{Q}_p(\alpha)$). One can do this (see [BPR93], or [SW13]) by defining preliminary height functions h'_ω and $h'_{x\omega}$, and then extending linearly, i.e. given $\nu = a\omega + bx\omega$, let $h'_\nu = ah'_\omega + bh'_{x\omega}$. Explicitly, we have $h'_\omega(P) = -\log_\omega(P)^2$, where \log_ω is the logarithm associated to ω . The definition of $h'_{x\omega}$ involves the σ -functions of either Mazur and Tate or of Bernardi. We refer to [SW13, Section 4] for an explicit definition, since it won't be needed in this paper. We then normalize and put $h_\nu := \frac{h'_\nu}{\log_p(\gamma)}$.

Remark 4.4. The reason for this normalization is that p -adic L -functions $L_p(T)$ are classically thought of as functions of a variable s via the substitution $T = \gamma^{s-1} - 1$, cf. [MTT86, §II.13]. The original formulation of p -adic BSD then investigated the behavior of a particular $L_p(\gamma^{s-1} - 1)$ at $s = 1$. Note that

$$\frac{d^r}{ds^r} L_p(\gamma^{s-1} - 1)|_{s=1} = \frac{d^r}{dT^r} L_p(T) \Big|_{T=0} \cdot \log_p(\gamma)^r.$$

The bilinear form associated to this height function has values in \mathbb{Q}_p (resp. $\mathbb{Q}_p(\alpha)$):

$$\langle P, Q \rangle_\nu = \frac{1}{2} (h_\nu(P + Q) - h_\nu(P) - h_\nu(Q))$$

Definition 4.5. Let Reg_ν be the discriminant of this height pairing on $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$.

Definition 4.6. Let ν_A and ν_B be as above. We define normalized height functions

$$\hat{h}_{\nu_A} := \frac{h_{\nu_A}}{[\nu_B, \nu_A]} = \frac{h_{\nu_A}}{[\omega, \nu_A]} \text{ and } \hat{h}_{\nu_B} := \frac{h_{\nu_B}}{[\nu_A, \nu_B]} = \frac{h_{\nu_B}}{[\omega, \nu_B]},$$

and denote their corresponding regulators by $\text{Reg}_{\frac{1}{\alpha}}$ and $\text{Reg}_{\frac{1}{\beta}}$. Note that the height functions (and thus the regulators) are independent of the choice of our Weierstraß equation.

Denote by $r(E)$ the rank of $E(\mathbb{Q})$. In the supersingular case, Perrin-Riou defines the regulator $\text{Reg}_p^{BPR}(E/\mathbb{Q})$ as the unique element in $D_p(E)$ so that for any $\nu \in D_p(E)$ with $\nu \notin \mathbb{Q}_p\omega$, we have¹

$$(1) \quad [\text{Reg}_p^{BPR}(E/\mathbb{Q}), \nu] = \frac{\text{Reg}_\nu}{[\omega, \nu]^{r-1}} \text{ where } r = r(E) > 0.$$

For $r(E) = 0$, she puts $\text{Reg}_p^{BPR}(E/\mathbb{Q}) = \omega$.

Definition 4.7. As an element of $D_p(E)(\alpha)$, define

$$\text{Reg}_p(E/\mathbb{Q}) := (\text{Reg}_{\frac{1}{\beta}}, \text{Reg}_{\frac{1}{\alpha}}) \begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix}.$$

Proposition 4.8. We have $\text{Reg}_p^{BPR}(E/\mathbb{Q}) = \text{Reg}_p(E/\mathbb{Q}) \in D_p(E)$.

¹This characterization is that of [SW13, Lemma 4.2], which is a corrected version of Perrin-Riou's original lemma, [PR03, Lemme 2.6].

Proof. When $r(E) = 0$, this follows from the fact that $\text{Reg}_{\frac{1}{\alpha}} = 1$ and $\text{Reg}_{\frac{1}{\beta}} = 1$.

When $r(E) > 0$, note that

$$[\text{Reg}_p(E/\mathbb{Q}), \nu_A] = \text{Reg}_{\frac{1}{\alpha}} \cdot [\nu_B, \nu_A] = \frac{\text{Reg}_{\nu_A}}{[\nu_B, \nu_A]^{r-1}} = \frac{\text{Reg}_{\nu_A}}{[\omega, \nu_A]^{r-1}},$$

and similarly, $[\text{Reg}_p(E/\mathbb{Q}), \nu_B] = \frac{\text{Reg}_{\nu_B}}{[\omega, \nu_B]^{r-1}}$. Since ν_A and ν_B form a basis for $D_p(E)(\alpha)$, linearity tells us that the property described in equation (1) holds for any $\nu \in D_p(E)(\alpha)$.

Now suppose that $\Delta := \text{Reg}_p(E/\mathbb{Q}) - \text{Reg}_p^{BPR}(E/\mathbb{Q}) \neq 0$. Then

$$[\Delta, \nu] = 0 \text{ for any } \nu \in D_p(E),$$

so this would in particular hold for $\nu = \omega$ or $\nu = x\omega$, from which we conclude by linearity that

$$[\Delta, \nu] = 0 \text{ for any } \nu \in D_p(E)(\alpha).$$

But this would imply $\Delta = 0$.

Q.E.A.

4.2. Statement of the conjectures. The following is a p -adic analogue of the Birch and Swinnerton-Dyer conjectures when p is supersingular (cf. [BPR93, Conjecture on page 229] and [PR03, Conjecture 2.5]):

Conjecture 4.9 (Bernardi and Perrin-Riou). *Let p be a good supersingular prime, and denote by r^{an} the order of vanishing of $L_p^{PR}(E, T)$ at 0, and by $L_p^{PR*}(E)$ its leading coefficient (with value in the Dieudonné module) of its Taylor expansion around 0.*

(1) *We have $r^{an} = r(E)$.*

(2) $L_p^{PR*}(E) = (1 - \varphi)^2 \frac{\prod_v c_v \cdot \#\text{III}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2} \text{Reg}_p(E/\mathbb{Q})$.

Remark 4.10. Note that while the objects in the second part of this conjecture depend on the choice of Weierstraß equation, their coordinates with respect to the basis $\{\nu_\alpha, \nu_\beta\}$ don't. In fact, one can formulate Bernardi's and Perrin-Riou's conjecture in a form that resembles more closely that of the one given by Mazur, Tate, and Teitelbaum:

Conjecture 4.11 (Equivalent formulation of above). *Let r^{an} be as in Lemma 4.12 below, and L_α^* and L_β^* be the leading coefficients in the Taylor expansion. Then*

(1) $r^{an} = r(E)$.

(2) $L_\alpha^* = (1 - \frac{1}{\alpha})^2 \frac{\prod_v c_v \cdot \#\text{III}(E/\mathbb{Q}) \cdot \text{Reg}_{\frac{1}{\beta}}}{(\#E(\mathbb{Q})_{tors})^2}$, and $L_\beta^* = (1 - \frac{1}{\beta})^2 \frac{\prod_v c_v \cdot \#\text{III}(E/\mathbb{Q}) \cdot \text{Reg}_{\frac{1}{\alpha}}}{(\#E(\mathbb{Q})_{tors})^2}$.

This version can be found in [Co04, Conjecture 0.12], where it is attributed to Mazur, Tate and Teitelbaum.

Lemma 4.12. *Since p is supersingular, $r^{an} := \text{ord}_{T=0} L_p(E, \alpha, T) = \text{ord}_{T=0} L_p(E, \beta, T)$.*

Proof. The same proof as in [Po03, Lemma 6.6] works.

4.3. A version of the conjectures via L_{\sharp} and L_{\flat} in the supersingular case. We now reformulate Conjecture 4.9 using L_{\sharp} and L_{\flat} .

Definition 4.13. We call $\vec{L}_p(E, T) := \vec{L}_p := (L_{\sharp}, L_{\flat})$ the p -adic L -vector of E , and denote by r_p^{\natural} the minimum of the orders of vanishing of L_{\sharp} and L_{\flat} .

We would now like to find a pair of elements ν_{\sharp} and ν_{\flat} in $D_p(E)$ that give rise to regulators corresponding to our p -adic L -functions. Recall that $L_p^{PR}(E, T) = (L_{\sharp}, L_{\flat}) \mathcal{L}og_{\alpha, \beta} \begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix}$.

Definition 4.14. Let $Z := \mathcal{L}og_{\alpha, \beta}(1 + T)|_{T=0} = \mathcal{L}og_{\alpha, \beta}(1)$. We define

$$\begin{pmatrix} \nu_{\sharp} \\ \nu_{\flat} \end{pmatrix} := Z \begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix},$$

$$(N_{\sharp}, N_{\flat}) := (\nu_B, -\nu_A) \begin{pmatrix} (1-\frac{1}{\alpha})^2 & 0 \\ 0 & (1-\frac{1}{\beta})^2 \end{pmatrix} Z^{-1} \times \det Z.$$

Lemma 4.15. $\nu_{\sharp}, \nu_{\flat}, N_{\sharp}, N_{\flat}$ are in $D_p(E)$ and are not \mathbb{Q}_p -multiples of ω .

Proof. Calculation.

Definition 4.16. We let $\text{Reg}_{\sharp} := \text{Reg}_{\frac{N_{\sharp}}{[\omega, N_{\sharp}]}}$ and $\text{Reg}_{\flat} := \text{Reg}_{\frac{N_{\flat}}{[\omega, N_{\flat}]}}$ be the regulators for the normalized heights associated to N_{\sharp} and N_{\flat} . Also, we let

$$\text{Reg}_p^{\natural} := \begin{cases} \begin{pmatrix} (-a_p^2 + 2a_p + p - 1)\text{Reg}_{\sharp}, & (-a_p + 2)\text{Reg}_{\flat} \end{pmatrix} & \text{for odd } p, \\ \begin{pmatrix} (-a_p^3 + 2a_p^2 + 2pa_p - a_p - 2p)\text{Reg}_{\sharp}, & (-a_p^2 + 2a_p + p - 1)\text{Reg}_{\flat} \end{pmatrix} & \text{for even } p. \end{cases}$$

We are now ready to give our p -adic version of BSD:

Conjecture 4.17 (Tandem p -adic BSD). *Let E be an elliptic curve and p a prime of good supersingular reduction. Denote by \vec{L}_p^* the first non-zero leading Taylor coefficient around $T = 0$ of $\vec{L}_p = \vec{L}_p(E, T)$.*

- (1) We have $r_p^{\natural} = r(E)$.
- (2) $\vec{L}_p^* = \frac{\prod_v c_v \cdot \#\text{III}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\text{tors}})^2} \text{Reg}_p^{\natural}(E/\mathbb{Q})$

Remark 4.18. The term $\text{Reg}_p^{\natural}(E/\mathbb{Q})$ is independent from the choice of Weierstraß equation. This follows from the proof of part 2 of Theorem 4.19, which only compares *coordinates* with respect to the basis $\nu_{\alpha}, \nu_{\beta}$.

Theorem 4.19. *This conjecture is equivalent to that of Bernardi and Perrin-Riou (i.e. Conjecture 4.9).*

Definition 4.20. Let $r = r(E) > 0$. Given a vector $\nu \in D_p(E)$ (or in $D_p(E)(\alpha)$) that is not a linear multiple of ω , we put

$$\widetilde{\text{Reg}}_{\nu} := \frac{\text{Reg}_{\nu}}{[\omega, \nu]^{r-1}}.$$

Remark 4.21. We know that $\widetilde{\text{Reg}}_\nu$ is linear in ν . See e.g. [SW13, proof of Lemma 4.2].

Proof of equivalence for part 1. This follows from Lemma 4.12 and the product rule. Q.E.D.

Proof for part 2. From the equivalence of part 1 and the product rule, we have

$$\vec{L}_p^* \mathcal{L}og_{\alpha, \beta}(1) = \vec{L}_p^* Z = (L_\alpha^*, L_\beta^*).$$

But we also have, for $r > 0$,

$$(1 - \varphi)^2 (\text{Reg}_{\frac{1}{\beta}}, \text{Reg}_{\frac{1}{\alpha}}) \begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix} = \left(\frac{\widetilde{\text{Reg}}_{\nu_B}}{[\omega, \nu_B]}, \frac{\widetilde{\text{Reg}}_{\nu_A}}{[\omega, \nu_A]} \right) \begin{pmatrix} (1 - \frac{1}{\alpha})^2 & 0 \\ 0 & (1 - \frac{1}{\beta})^2 \end{pmatrix} Z^{-1} \begin{pmatrix} \nu_\sharp \\ \nu_b \end{pmatrix}.$$

Since $[\omega, \nu_B] = [\nu_A, \nu_B] = -[\omega, \nu_A]$ and $\widetilde{\text{Reg}}_\nu$ is linear in ν , and by Lemma 4.15, this is equal to

$$\frac{1}{\det Z} \left(\frac{1}{[\nu_A, \nu_B]} \widetilde{\text{Reg}}_{N_\sharp}, \frac{-1}{[\nu_A, \nu_B]} \widetilde{\text{Reg}}_{N_b} \right) \begin{pmatrix} \nu_\sharp \\ \nu_b \end{pmatrix}.$$

But $\widetilde{\text{Reg}}_{N_\sharp} = [\omega, N_\sharp] \text{Reg}_\sharp$, so this is equal to

$$\left(\frac{[\omega, N_\sharp]}{[\nu_\sharp, \nu_b]} \text{Reg}_\sharp, \frac{-[\omega, N_b]}{[\nu_\sharp, \nu_b]} \text{Reg}_b \right) \begin{pmatrix} \nu_\sharp \\ \nu_b \end{pmatrix}.$$

The rest follows from explicit calculation of the factors preceding the regulators. Q.E.D.

What is known so far is the following theorem of Kato:

Theorem 4.22 ([Ka04], cf. [Ko03, Theorem 9.4] when $a_p = 0$). *In Conjectures 4.17, 4.11, 4.9, and 4.23, the orders of vanishing of the p -adic L -functions are all $\geq r(E)$.*

4.4. A remark in the ordinary case. *When p is ordinary, there is the following conjecture of Mazur, Tate, and Teitelbaum.*

Conjecture 4.23 (Mazur, Tate, and Teitelbaum). *Let p be a good ordinary prime, and denote by r^{an} the order of vanishing of $L_p(E, \alpha, T)$ at 0, and by $L_p^*(E)$ the leading coefficient of the Taylor expansion at 0.*

(1) *We have $r^{an} = r(E)$.*

(2) $L_p^*(E) = (1 - \frac{1}{\alpha})^2 \frac{\prod_v c_v \cdot \# \text{III}(E/\mathbb{Q}) \cdot \text{Reg}_{\frac{1}{\beta}}(E/\mathbb{Q})}{(\# E(\mathbb{Q})_{tors})^2}.$

Remark 4.24. These conjectures are a combination of [MTT86, §II.10, Conjecture (BSD(p))], which asserts that $r^{an} \geq r(E)$, and the remark thereafter, which predicts the non-vanishing of $\text{Reg}_{\frac{1}{\beta}}(E/\mathbb{Q})$.

Remark 4.25. We encounter the term $\text{Reg}_{\frac{1}{\beta}}$ (rather than $\text{Reg}_{\frac{1}{\alpha}}$) because of our choice of Frobenius $\varphi = \frac{F}{p}$, where F is the Frobenius as chosen in [MST06] or [Ke01]. The regulator comes from the normalized height associated to the unit-eigenvector α of F on $D_p(E)$, so that the eigenvalue for φ becomes $\frac{\alpha}{p} = \frac{1}{\beta}$.²

²In [SW13, Section 4.1], the regulator was accidentally constructed from the height coming from the normalized eigenvector of φ with eigenvalue $\frac{1}{\alpha}$. Everything works in that section if one replaces α by β .

In the ordinary case, recall that L_{\sharp} and L_{\flat} are not well-defined, but their values at $T = 0$ are. In particular this means that when $a_p = 2$ and p is odd, we may have $L_{\flat}(E, 0) = 0$ while $L(E, 1) \neq 0$, reminiscent of an extra zero phenomenon. This leads us to ask:

Question 2. *Where does this extra-zero phenomenon come from?*

5. THE GREATEST COMMON DIVISOR

We now generalize and give some evidence for the following conjecture found in [KP07, Problem 3.2].

Recall that d_n denoted the normalized jump in the ranks at the n th level of the cyclotomic tower:

$$d_n = \frac{1}{p^n - p^{n-1}} (\text{rank} E(\mathbb{Q}_n) - \text{rank} E(\mathbb{Q}_{n-1}))$$

Conjecture 5.1 (The problem of Kurihara and Pollack). *Let E/\mathbb{Q} be an elliptic curve so p is an odd prime of good supersingular reduction and $a_p = 0$. Then*

$$\gcd(L_{\sharp}(E, T), L_{\flat}(E, T)) = \left(T^r \prod_{d_n \geq 1 \text{ and } n \geq 1} \Phi_{p^n}^{d_n-1}(1+T) \right).$$

Note that this is an equality of *ideals*, since the greatest common divisor of two functions of $\mathbb{Q} \otimes \mathbb{Z}_p[[T]]$ is only well-defined as a $\mathbb{Z}_p[[T]]$ -ideal. We can give the following proposition:

Proposition 5.2. *Let E/\mathbb{Q} be an elliptic curve and p a prime of good supersingular reduction. For some polynomial $P_{\text{III}}(E, T)$ with $P_{\text{III}}(E, \zeta_{p^n} - 1) \neq 0$ for $n \geq 0$,*

$$\gcd(L_{\sharp}(E, T), L_{\flat}(E, T)) = \left(P_{\text{III}}(E, T) \cdot T^{r^{an}} \prod_{d_n \geq 1 \text{ and } n \geq 1} \Phi_{p^n}^{\epsilon_n^{an}-1}(1+T) \right),$$

where $\epsilon_n^{an} - 1 = d_n^{an} - 1$ or $\epsilon_n^{an} - 1 = d_n^{an}$.

Convention 5.3. Given a vector $(f(T), g(T))$ of p -adic analytic functions, we define its order of vanishing at s by $\text{ord}_{T=s}(f(T), g(T)) := \min(\text{ord}_{T=s} f(T), \text{ord}_{T=s} g(T))$.

Lemma 5.4. *Denote by ι (any) complex conjugation. Let $f(T), g_1(T), g_2(T)$, and the entries of a 2×2 matrix $M(T)$ be p -adic analytic functions on the open unit disc and $e = \text{ord}_{T=s} f(T)$ so that*

$$(f(T), \iota(f(T))) = (g_1(T), g_2(T))M(T)$$

and $\det M(s) \neq 0$. Then we have $\text{ord}_{T=s}(g_1(T), g_2(T)) = e$.

Proof. By calculus, $(f^{(m)}(s), \iota(f^{(m)}(s))) = (0, 0)$ if and only if $(g_1^{(m)}(s), g_2^{(m)}(s)) = (0, 0)$ for $m \geq 0$. Q.E.D.

Corollary 5.5. *The exact power of T dividing $\gcd(L_{\sharp}(E, T), L_{\flat}(E, T))$ is $T^{r^{an}}$.*

Lemma 5.6. *Let $\vec{f}(T) = (f_1(T), f_2(T))$ and $\vec{g}(T) = (g_1(T), g_2(T))$ be vectors of analytic functions on the open unit disc satisfying*

$$\vec{f}(T) = \vec{g}(T)\mathcal{C}_n, \text{ where } \mathcal{C}_n = \begin{pmatrix} a_p & p \\ -\Phi_{p^n}(1+T) & 0 \end{pmatrix}.$$

Let $s = \zeta_{p^n} - 1$. Then $\text{ord}_{T=s}\vec{g}(T) = \text{ord}_{T=s}\vec{f}(T)$ or $\text{ord}_{T=s}\vec{g}(T) = \text{ord}_{T=s}\vec{f}(T) - 1$.

Proof. Since $\text{ord}_{T=s}g_1(T) = \text{ord}_{T=s}f_2(T)$ and $a_pg_1(T) - f_1(T) = -\Phi_{p^n}(1+T)g_2(T)$,

$$\begin{cases} \text{ord}_{T=s}f_1(T) < \text{ord}_{T=s}f_2(T) & \text{implies } \text{ord}_{T=s}g_2(T) = \text{ord}_{T=s}f_1(T) - 1, \\ \text{ord}_{T=s}f_1(T) = \text{ord}_{T=s}f_2(T) \text{ and } a_p \neq 0 & \text{implies } \text{ord}_{T=s}g_2(T) \geq \text{ord}_{T=s}f_1(T) - 1, \\ \text{ord}_{T=s}f_1(T) > \text{ord}_{T=s}f_2(T) \text{ and } a_p \neq 0 & \text{implies } \text{ord}_{T=s}g_2(T) = \text{ord}_{T=s}f_2(T) - 1, \\ \text{ord}_{T=s}f_1(T) \geq \text{ord}_{T=s}f_2(T) \text{ and } a_p = 0 & \text{implies } \text{ord}_{T=s}g_2(T) = \text{ord}_{T=s}f_1(T) - 1. \end{cases}$$

Q.E.D.

Proof of Proposition 5.2. We use Corollary 5.5 and the following argument: Let $\mathcal{M} = I$ when $n = 1$ and $\mathcal{M} = \mathcal{C}_1 \cdots \mathcal{C}_{n-1}$ when $n > 1$. Recall that $\vec{L}_p = (L_\sharp(E, T), L_\flat(E, T))$, so that

$$(L_p(E, \alpha, T), L_p(E, \beta, T)) = \vec{L}_p \mathcal{M} \mathcal{C}_n \Xi_n$$

for some 2×2 matrix Ξ_n so that $\det \Xi_n(\zeta_{p^n} - 1) \neq 0$. From Lemma 5.4, $\text{ord}_{T=\zeta_{p^n}-1}(\vec{L}_p \mathcal{M} \mathcal{C}_n) = d_n^{an}$. Lemma 5.6 then implies

$$\text{ord}_{T=\zeta_{p^n}-1}(\vec{L}_p \mathcal{M}) = d_n^{an} - 1 \text{ or } \text{ord}_{T=\zeta_{p^n}-1}(\vec{L}_p \mathcal{M}) = d_n^{an}.$$

From $\det \mathcal{M}(\zeta_{p^n} - 1) \neq 0$ and Lemma 5.4 again, $\text{ord}_{T=\zeta_{p^n}-1}\vec{L}_p = d_n^{an} - 1$ or $\text{ord}_{T=\zeta_{p^n}-1}\vec{L}_p = d_n^{an}$.
Q.E.D.

In view of the problem of Kurihara and Pollack (Conjecture 5.1), we make the following conjecture:

Conjecture 5.7. *Let E/\mathbb{Q} be an elliptic curve, and p a good supersingular prime. Then*

$$\gcd(L_\sharp(E, T), L_\flat(E, T)) = \left(T^r \prod_{d_n \geq 1 \text{ and } n \geq 1} \Phi_{p^n}^{d_n-1}(1+T) \right).$$

REFERENCES

- [BPR93] D. Bernardi, B. Perrin-Riou: *Variante p -adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier)*, Comptes Rendus de l'Académie des Sciences. Paris Série I Mathématique **317** (1993), no. 3, 227-232.
- [KP07] M. Kurihara, R. Pollack: *Two p -adic L -functions and rational points on elliptic curves with supersingular reduction*, L -functions and Galois representations, 300-332.
- [Co04] Colmez, P.: *La conjecture de Birch et Swinnerton-Dyer p -adique*, Astérisque **294**, ix (2004), 251-319.
- [Ka04] K. Kato: *p -adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117-290.

- [Ke01] K. Kedlaya: *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, Journal of the Ramanujan Mathematical Society, **16** (2001), no. 4, 323-338.
- [Ko03] S. Kobayashi: *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no.1, 1-36.
- [LZ13] D. Loeffler, S. Zerbes, J. Reine Angew. Math., 679 (2013), p. 181 - 206.
- [MST06] B. Mazur, W. Stein, J. Tate: *Computation of p -adic heights and log convergence*, Doc. Math. 2006, Extra Vol., 577-614.
- [MTT86] B. Mazur, J. Tate, and J. Teitelbaum: *On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1-48.
- [PR03] B. Perrin-Riou: *Arithmétique des courbes elliptiques à réduction supersingulière*. Experiment. Math. **12** (2003), 155-186.
- [Po03] R. Pollack: *The p -adic L -function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 1, 1-36.
- [Sil] J. Silverman: *The arithmetic of elliptic curves*, Second Edition, Graduate Texts in Mathematics **106** (2009), Springer, New York.
- [Sp12] F. Sprung: *Iwasawa Theory for elliptic curves at supersingular primes: A pair of Main Conjectures*, Journal Of Number Theory **132** (2012), no. 7.
- [Sp13] F. Sprung: *The Šafarevič-Tate group of an elliptic curve in cyclotomic \mathbb{Z}_p -extensions at supersingular primes* J. Reine Angew. Math., **681** (2013), August 2013.
- [Sp15] F. Sprung: *On pairs of p -adic L -functions for weight two modular forms*, Submitted.
- [Sp16] F. Sprung: *The rank of an elliptic curve in cyclotomic \mathbb{Z}_p -extensions at supersingular primes*, in preparation.
- [SW13] W. Stein, C. Wuthrich: *Algorithms for the Arithmetic of Elliptic Curves using Iwasawa Theory*, Mathematics of Computation, **82** (2013), 1757-1792.

Florian Sprung, Princeton University and the Institute for Advanced Study, Princeton, NJ.
email: fsprung@math.princeton.edu